Información Tecnológica
Vol. 23(3), 113-120 (2012)
doi: 10.4067/S0718-07642012000300014

# Metodología para la Detección de Vulnerabilidades en Redes de Datos

**David A. Franco, Jorge L. Perea y Plinio Puello**
Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA, Avenida del Consulado, Calle 30, No. 48 – 152, Cartagena-Colombia. (e-mail: dfrancob@unicartagena.edu.co, jochyone@gmail.com, ppuellom@unicartagena.edu.co).

*Recibido Sep. 08, 2011; Aceptado Oct. 21, 2011; Versión final recibida Dic. 20, 2011*

---

### Resumen

El objetivo principal de este trabajo fue diseñar una metodología para la detección de vulnerabilidades en redes de datos. Para esto se desarrollaron diferentes fases llamadas reconocimiento, escaneo de puertos y enumeración de servicios, y escaneo de vulnerabilidades, cada una de las cuales es soportada por herramientas de software. Los resultados de cada fase suministran datos necesarios para la ejecución de las siguientes etapas. Con el fin de validar la utilidad de la metodología propuesta se llevó a cabo su implementación en la red de datos de la Universidad de Cartagena en Colombia, encontrando diferentes tipos de vulnerabilidades. Finalmente apoyándose en los resultados obtenidos, se encontró que la metodología propuesta es de gran utilidad para detectar vulnerabilidades en redes de datos, lo que demuestra su importancia para el área de la seguridad informática.

*Palabras clave: detección de vulnerabilidades, enumeración de servicios, escaneo de puertos, seguridad informática*

# Methodology for Detecting Vulnerabilities in Data Networks

### Abstract

The main objective of this study was to design a methodology for the detection of vulnerabilities in data networks. This involved the development of different phases, called recognition, port scanning and service enumeration, and vulnerability scanning, each of which is supported by software tools. The results of each phase supplied the necessary data for implementing the following stages. To validate the usefulness of the proposed methodology this was implemented in the data network of the University of Cartagena in Colombia, finding different types of vulnerabilities. Finally, based on the results, it was found that the proposed methodology is useful for detecting vulnerabilities in data networks, demonstrating their importance to the area of computer security.

*Keywords: vulnerability detection, service enumeration, port scanning, information security*

## INTRODUCCIÓN

En la actualidad existen diferentes proyectos que tienen como finalidad encontrar vulnerabilidades en diferentes tipos de plataformas, entre los más importantes para este estudio podemos mencionar que en el campo de las aplicaciones Web sobresalen NeXpose (también útil para plataformas de escritorio), acunetix, w3af, entre otros. Algunos de estos proyectos han sido examinados en trabajos de investigación (Bau et al., 2010) donde se evaluaron ocho diferentes escáneres de vulnerabilidades de aplicaciones web, con el fin de determinar su efectividad en la detección de éstas. Además, otro trabajo (Shi et al., 2010) realizó la evaluación de diferentes herramientas de seguridad, a la vez que se compararon las habilidades de las mismas. Por otro lado, otros trabajos (Hadavi et al., 2008; Qualys, 2009; Mell et al., 2007; Huan et al., 2010; Yun-hua y Pei, 2010; Harada et al., 2010; Jensen et al., 2008; Wren et al., 2010; Al-Fedaghi, 2010; Kuhn y Johnson, 2010; García y Vázquez, 2005) buscan aportar al avance de la investigación relacionada con las vulnerabilidades en seguridad informática.

Pese a los trabajos que han sido realizados el problema que surge de la presencia de vulnerabilidades en redes de datos, sigue causando grandes pérdidas a organizaciones e individuos en la actualidad, por esto se han desarrollado diferentes metodologías para la detección de dichas vulnerabilidades (Watanabe et al., 2010). En este artículo se presenta una metodología para la detección de vulnerabilidades en redes de datos, de fácil uso y soportado integralmente en herramientas software, dicha metodología presenta un enfoque práctico y conceptual para la detección y erradicación de vulnerabilidades. Adicionalmente se presenta un caso de estudio de aplicación de la metodología propuesta, mediante el cual se logra establecer la utilidad y funcionalidad de esta.

## TRABAJOS RELACIONADOS

Romero et al. (2009) presentan una herramienta metodológica para identificar los activos relevantes en un proceso de identificación de riesgo en aplicaciones web, para soportar el instrumento metodológico propuesto se implementa un caso de estudio y se realiza un análisis cuantitativo y cualitativo del mismo; sin embargo, este trabajo se limita a la identificación de activos expuestos a riesgos y no propone mecanismos para la detección del peligro al que dichos activos están expuestos, es decir, no propone mecanismos para la detección de las vulnerabilidades de estos activos. Por otro lado Pfleeger y Ciszek (2008), proponen una metodología de cuatro pasos que pretende ayudar a las organizaciones a evaluar los activos relevantes a ser protegidos, determinar los potenciales atacantes y los posibles métodos para disminuir el riesgo, sin embargo, no se precisan técnicas para evaluación de la seguridad de dichos activos, por lo que da lugar a proteger elementos que no tienen riesgos. De forma similar se propone una metodología (Xinlan et al., 2010) para evaluar el riesgo de seguridad de la información, pero está basada en un análisis matemático y no aporta herramientas para evaluar el grado de vulnerabilidad de un activo dentro de una organización. En otro trabajo (Ruiz et al., 2009) se propone una metodología de cinco pasos para ayudar a disminuir los problemas de seguridad en las pequeñas y medianas empresas mexicanas, no obstante, dicha metodología no proporciona mecanismos concretos para la detección de vulnerabilidades y limita su alcance a cierto tipo de organizaciones de un país concreto, mientras que la metodología que se propone en el presente artículo puede ser aplicada a cualquier tipo de organización con independencia del país en el que se encuentre. Debido a que los trabajos citados anteriormente carecen ya sea, de mecanismos para la detección del riesgo de los activos de una organización, de herramientas que permitan encontrar vulnerabilidades o presentan un enfoque que impide su uso en organizaciones de distintos niveles de complejidad, existe la necesidad de metodologías que tengan en cuenta estos aspectos, por lo anterior en el presente artículo se propone una metodología para la detección de vulnerabilidades en redes de datos equipada con los elementos necesarios para atender los requisitos planteados anteriormente.

## METODOLOGÍA PARA LA DETECCIÓN DE VULNERABILIDADES EN REDES DE DATOS

La metodología para la detección de vulnerabilidades en redes de datos que se propone en este artículo, consta de tres fases soportadas por herramientas de software, mediante las cuales se busca obtener las vulnerabilidades en los equipos de red (tanto cableada como inalámbrica) y servidores en las redes de datos objeto de estudio (en adelante: red objetivo). Esta metodología se diferencia de otras en la medida en que se soporta cada etapa en herramientas software. Por lo que en cada fase se puntualizan las acciones que se deben realizar y cómo se deben llevar a cabo a través de las herramientas apropiadas. El esquema de la metodología para detección de vulnerabilidades en redes de datos, se presenta en la figura 1. Como puede verse en esta figura, la metodología propuesta consta de tres fases, las cuales se detallan a continuación.

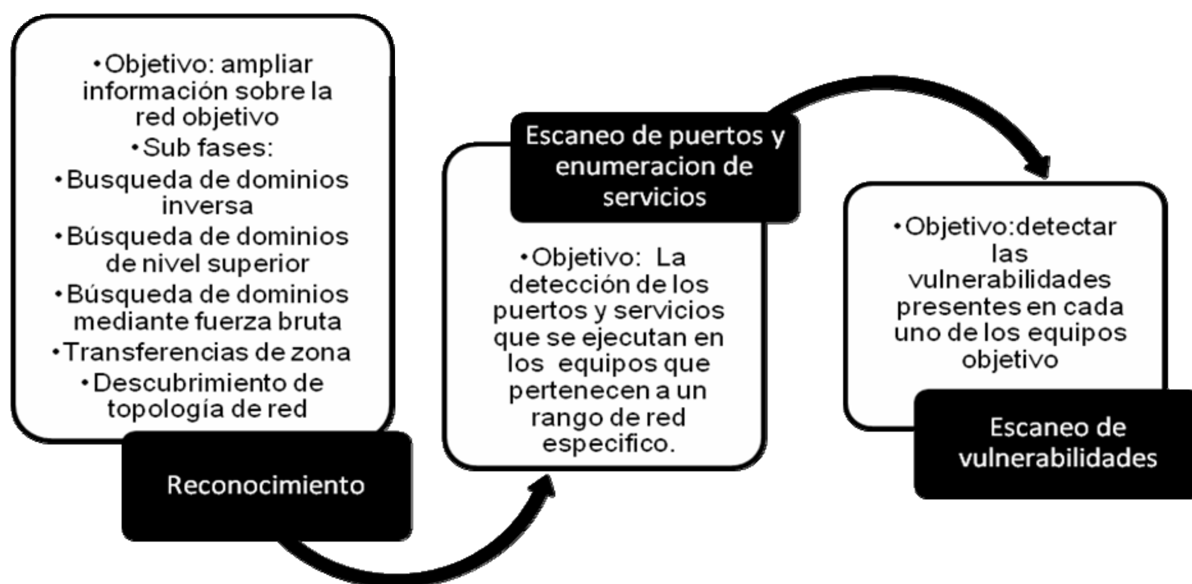



Fig. 1: Esquema de la metodología para la detección de vulnerabilidades en redes de datos.

La figura anterior muestra cada una de las fases que deben llevarse a cabo. La primera fase consiste en obtener tanta información como sea posible de la red objetivo, para esto se realizan implementan técnicas que se basan en diferentes tipos de consultas a servidores DNS y técnicas que se basan en el análisis de los mensajes de enrutamiento. Se resalta que esta fase no busca obtener vulnerabilidad alguna, lo que se pretende con ella es obtener una lista lo más amplia posible sobre los equipos con presencia en internet de la red objetivo. Dicha lista de equipos de red es utilizada en la segunda fase llamada escaneo de puertos y enumeración de servicios, en esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos. Dependiendo del tipo de puerto y servicio que este activo en cada equipo se puede inferir el rol que este juega dentro de la organización. Nuevamente se anota que en esta fase no se pretende encontrar vulnerabilidad alguna, sino determinar los equipos críticos de la red objetivo a los cuales se les aplicará el escaneo de vulnerabilidades, que constituye la fase final de esta metodología. Una vez obtenida la lista de los equipos de la red objetivo con presencia en internet y habiendo determinado cuáles de ellos juegan un rol crítico para la red, se procede con la fase final de la metodología propuesta. La cual evaluará a los equipos críticos en busca de vulnerabilidades. Es en esta última fase en la que se realiza la evaluación de todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.

El número total de vulnerabilidades evaluadas puede ascender hasta el total registrado en el repositorio de vulnerabilidades de los Estados Unidos (base de datos nacional de vulnerabilidades, NVD por sus siglas en inglés), la cual desde 2002 reúne la información de todas las vulnerabilidades reportadas (en el momento de escribir este artículo el número ascendía a 48620) y se mantiene en actualización diaria con una tasa media de 10 vulnerabilidades nuevas

diariamente (NIST, 2011). El hecho de que se pueda evaluar hasta la totalidad de las vulnerabilidades reportadas en la NVD es posible debido a que la herramienta sugerida para llevar a cabo esta fase de la metodología utiliza dicha base de datos para realizar la búsqueda de vulnerabilidades, esto además permite que se puedan evaluar la mayoría de los servicios que se ejecutan en un equipo de cómputo.

Se sugiere utilizar la versión 4r2 de la distribución de Linux BackTrack, que fue el sistema operativo que se utilizó al momento de implementar la metodología propuesta, esta distribución contiene pre-instaladas la mayoría de las herramientas que la soportan. Adicionalmente las guías expuestas a continuación se realizan teniendo en cuenta esta distribución.

*Fase I: Reconocimiento (recolección de información)*

Esta fase tiene como objetivo obtener y ampliar información sobre la red objetivo a partir de su nombre de dominio. Principalmente se pretende ampliar el número de equipos de cómputo (en adelante: equipos) que se evaluarán posteriormente. Para ello se realizará lo siguiente: búsqueda de nombres de dominio a partir de direcciones IP, búsqueda de dominios de nivel superior, búsqueda de dominios mediante fuerza bruta, transferencias de zona, descubrimiento de topología de red. Cabe resaltar que en esta fase no se busca encontrar ninguna vulnerabilidad en absoluto, lo que se pretende es obtener la mayor cantidad posible de equipos que la red objetivo tiene con presencia en internet.

Búsqueda de dominios inversa**:** El objetivo de esta sub fase es encontrar nombres de dominios relacionados con el dominio objetivo y que se encuentren en el mismo segmento de red, es decir, una vez determinada la dirección IP del dominio objetivo (esta dirección puede obtenerse mediante el comando ping), se buscará en el segmento IP/24 aquellos nombres de dominio que tengan relación con el dominio principal. Esta búsqueda es soportada por la herramienta dnsrecon (ubicado en BT 4-R2 bajo la ruta /pentest/enumeration/dnsrecon). Con lo anterior se suman equipos potenciales para posterior evaluación. La ejecución de esta herramienta suministrará todos los dominios registrados a las direcciones IP en el rango del dominio objetivo, con lo que se podrá detectar cuáles de ellos pertenecen o tienen relación con este, lo cual amplía la lista de equipos que se evaluarán posteriormente.

Búsqueda de dominios de nivel superior: Esta búsqueda permite detectar dominios de nivel superior (ejemplo de tales dominios: .com, .net, .org) asociados al nombre de dominio objetivo. En caso de que se encuentre un dominio de nivel superior asociado al dominio objetivo, este se incluirá a la lista de equipos que se evaluarán en la fase siguiente. La búsqueda descrita anteriormente es soportada por la herramienta dnsrecon.

Búsqueda de dominios mediante fuerza bruta: Esta búsqueda permite hallar subdominios del dominio principal objetivo, mediante fuerza bruta. Subdominios como ftp.dominio, smtp.dominio, entre otros, son el objetivo de esta etapa. Una vez más si se detecta un subdominio relacionado con la red objetivo se someterá a evaluación en la fase siguiente. Por otro lado se anota que la herramienta dnsrecon también soporta esta etapa.

Transferencias de zona: Consiste en realizar consultas a los servidores de nombres de dominios encargados del dominio objetivo. Esto permitirá conocer subdominios o dominios relacionados con este último. Cabe señalar que esta técnica se aprovecha de la mala gestión de servidores DNS, que no se configuran para impedir que compartan base de datos de dominios con equipos diferentes de otros servidores DNS. El soporte de esta etapa es la herramienta dnsenum.

Descubrimiento de topología de red: En algunos casos, la evaluación de seguridad se realiza desde el interior de la red objetivo, en dichas situaciones es posible determinar la topología completa de la red mediante la escucha pasiva realizada con un sniffer. Esto permitirá capturar la información del protocolo de enrutamiento concerniente a las subredes que conforman la topología. Se resalta que esta técnica es posible debido a la mala configuración de los administradores de redes de sus equipos activos, puesto que la mayoría de estos últimos tienen

funciones para evitar la propagación de mensajes de enrutamiento a nodos terminales. Luego el funcionamiento de esta subetapa deja en evidencia una débil administración de la red. Para soportar esta técnica se utiliza la herramienta wireshark mediante la iniciación de su función para escuchar pasivamente a través de una interfaz de red específica.

*Fase II: Escaneo de puertos y enumeración de servicios*

De la ejecución de la fase anterior se obtiene una lista de todos los equipos que la red objetivo tiene con presencia en internet. En la fase actual se examinarán los puertos y servicios de cada uno de estos equipos y con base en el tipo de servicios que ofrecen, se realizará inferencia sobre el papel que cada uno juega dentro de la red objetivo, así como también la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales). Adicionalmente la información obtenida de la fase anterior también es útil para realizar una evaluación indiscriminada de todos los segmentos de red de una organización objeto de análisis. La herramienta que brinda soporte a esta etapa es NMAP. Es importante indicar que en esta fase no se pretende encontrar vulnerabilidad alguna, sino determinar los equipos críticos de la red objetivo a los cuales se les aplicará el procedimiento que se describe en la fase de la siguiente sección.

*Fase III: Escaneo de vulnerabilidades*

La fase anterior proporciona una lista de equipos que se consideran críticos o sensibles para la red objetivo, este subconjunto de equipos fue obtenido de un conjunto más grande (el conjunto de todos los equipos que la red objetivo tiene con presencia en internet) mediante la ejecución de la primera fase de la metodología. Los equipos que se encontraron como críticos son los que finalmente se someterán a evaluación en esta última fase, en la que se procede a la utilización de un escáner de vulnerabilidades. Este tiene como objetivo detectar los potenciales riesgos al que están expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red objetivo. Para esta etapa se recomienda el uso del escáner de vulnerabilidades NeXpose, una vez descargado e instalado, se debe ingresar el equipo o conjunto de equipos o segmento de red a escanear (estos equipos se seleccionan a partir de la fase anterior), posteriormente este presenta la opción de generar reportes en los que se indican con amplia descripción cada una de las vulnerabilidades encontradas y se presentan sugerencias de solución. Se recomienda seguir el manual de usuario de la herramienta NeXpose para llevar a cabo el escaneo de vulnerabilidades. Finalmente se anota que este escáner de vulnerabilidades utiliza el repositorio de vulnerabilidades del gobierno de los Estados Unidos, con lo que se garantiza que en todo momento las vulnerabilidades analizadas, son todas las que han sido reportadas hasta la actualidad.

## CASO DE ESTUDIO

La metodología anteriormente expuesta ha sido aplicada en la red de datos de la Universidad de Cartagena arrojando los resultados mencionados a continuación:

*Fase 1: Reconocimiento (recolección de información)*

Mediante la ejecución de esta fase se logró encontrar lo siguiente:

1. El nombre de dominio utilizado por la Universidad de Cartagena en internet.
2. El servidor de alojamiento de la Universidad y su dirección IP.
3. Dominios de nivel superior asociados con la Universidad.
4. Once subdominios de la forma X.unicartagena.edu.co.
5. Transferencia de zona contra los servidores de dominio de la Universidad, a través de la cual se detectaron 26 nuevos subdominios, de los cuales algunos se tomaron para las fases siguientes.
6. Detectar los segmentos de red de las diferentes sedes de la Universidad.

*Fase 2: Escaneo de puertos y enumeración de servicios*

A través de esta fase se encontró lo siguiente:

1. Se escanearon cada uno de los segmentos de red de la Universidad.
2. Se tabularon aquellos que presentaron servicios críticos como posibles candidatos de escaneo (29 servidores).
3. Se determinaron 18 como servidores críticos para posterior escaneo de vulnerabilidades.

*Fase 3: Escaneo de vulnerabilidades*

Es importante anotar que no se muestran los resultados detallados del caso de estudio, para proteger la integridad de la red de datos evaluada. A continuación un resumen de los resultados obtenidos con esta fase de la metodología:

1. El 83.33% de los servidores presentó vulnerabilidades críticas (requieren atención inmediata, ya que son fáciles de aprovechar por parte de los atacantes para obtener control total sobre el sistema) y severas (son más difíciles de explotar que las anteriores y no proveen el mismo nivel de acceso).

2. En el 100% de los servidores se encontraron vulnerabilidades moderada (proveen información a los atacantes para la ejecución de posteriores ataques. Su reparación no es tan urgente como en los casos anteriores).

3. Se logró establecer una categorización de las vulnerabilidades encontradas con relación a los servicios afectados por las mismas, por ejemplo: en el servidor "A" se detectaron "x" vulnerabilidades, de las cuales el "y"% afectan el servicio http, el "z"% afectan el servicio ftp, entre otros.

4. Se obtuvo solución para cada una de las vulnerabilidades encontradas.

Los resultados presentados arriba permitieron categorizar las vulnerabilidades encontradas, establecer el nivel de riesgo de cada una de ellas y brindar soluciones a las mismas. Lo cual demuestra que la metodología propuesta es de gran utilidad para la detección de vulnerabilidades en redes de datos.

## CONCLUSIONES

Este artículo presentó el desarrollo de una metodología para la detección de vulnerabilidades en redes datos. Dicha metodología se utilizó para la detección de vulnerabilidades al interior de la red de datos de la Universidad de Cartagena, proporcionando como resultado el hallazgo de diferentes problemas de seguridad. Basándose en los resultados obtenidos se concluye que la metodología propuesta: 1) Ayuda a encontrar de manera satisfactoria vulnerabilidades críticas, severas y moderadas en servidores que conforman redes de datos; 2) Permite la categorización de las vulnerabilidades encontradas, clasificándolas de acuerdo a los servicios afectados; 3) Es de gran utilidad teniendo un gran impacto en las organizaciones que deseen implementarla; y 4) De gran funcionalidad para hallar soluciones a estas vulnerabilidades por su fácil implementación.

## REFERENCIAS

Al-Fedaghi Sabah, System-based Approach to Software Vulnerability, socialcom: IEEE Second International Conference on Social Computing 2010, 1072-1079, (2010).

Bau J., Bursztein E., Gupta D., Mitchell J., State of the Art: Automated Black-Box Web Application Vulnerability Testing, 2010 IEEE Symposium on Security and Privacy, 332-345, (2010).

GARCIA, M.E. y VAZQUEZ, R., Arquitectura de un Billete Electrónico Anónimo: Medios Electrónicos de Pagos, Inf. tecnol, ISSN 0718-0764 (en línea), 16(3), 71-80 (2005), http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642005000300010&lng=es&nrm=iso. Acceso: 22 de Noviembre (2011).

Hadavi M.A., Sangchi H. M., Hamishagi V. S. y Shirazi H. Software Security; A Vulnerability-Activity Revisit, 2008 Third International Conference on Availability, Reliability and Security, 866-872, Marzo (2008).

Harada Toshiki, Kanaoka Akira, Okamoto Eiji y Kato Masahiko, Identifying Potentially-Impacted Area by Vulnerabilities in Networked Systems Using CVSS,2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, 367-370, (2010).

Huang Shuguang, Tang Heping, Zhang Min y Tian Jie, Text Clustering on National Vulnerability Database, 2010 Second International Conference on Computer Engineering and Applications, 295-299, (2010).

Jensen M., Gruschka N. y Luttenberger N., The impact of flooding attacks on network-based services, in Proceedings of the The Third International Conference on Availability, Reliability and Security, ARES 2008, IEEE Computer Society,509–513, Barcelona, España, Marzo (2008).

Kuhn Rick y JohnsonChris, Vulnerability Trends: Measuring Progress, IT Professional, 51-53, Julio (2010).

Mell P, Scarfone K. y Romanosky S, A Complete Guide to the Common Vulnerability Scoring System Version 2.0, Junio (2007).

National Institut of Standards and Tecnology., *National Vulnerability Database* (2011), http://nvd.nist.gov/. Acceso: 22 de Noviembre (2011).

Pfleeger S., Ciszek T., Choosing a Security Option: The InfoSecure Methodology, IT Professional, volumen 10, numero 5, 46-52, (2008).

QUALYS, The Top Cyber Security Risks Two risks dwarf all others, but organizations fail to mitigate them, Septiembre (2009).

Romero B., Haddad H. y Molero J., A Methodological Tool for Asset Identification in Web Applications: Security Risk Assessment, 2009 Fourth International Conference on Software Engineering Advances, 413-418, (2009).

Ruiz J., Ponce I., Díaz O., Zavala J., Zarate J. y Fuentes A., MISMA: An Approach to Mexican Information Security Methodology and Architecture for PYMES, conielecomp, 2009 International Conference on Electrical, Communications, and Computers, 65-68, (2009).

ShiH., Chen B. y YuL., Analysis of Web Security Comprehensive Evaluation Tools, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 285-289, (2010).

Watanabe Takanobu, Cheng Zixue, Kansen Mizuo y Hisada Masayuki, A New Security Testing Method for Detecting Flash Vulnerabilities by Generating Test Patterns,2010 13th International Conference on Network-Based Information Systems, 469-474, (2010).

Wren Chris, Reilly Denis y Berry Tom, Footprinting: A Methodology for Auditing eSystem Vulnerabilities, 2010 Developments in E-systems Engineering, 263-267, (2010).

Xinlan Zhang, Zhifang Huang, Guangfu Wei y Zhang Xin, Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarchy Process, 2010 Second WRI World Congress on Software Engineering, wcse, volumen 2, 157-160, (2010).

Yun-hua Gu y PeiLi, Design and Research on Vulnerability Database, 2010 Third International Conference on Information and Computing, 209-212, (2010).